TECNOLÓGICO DE MONTERREY®

Instituto Electoral Coahuila

Resumen Ejecutivo Auditoría PREP – Elecciones 2020

Resultados, hallazgos y recomendaciones de la auditoría al sistema del Programa Preliminar de Resultados Electorales del Instituto Electoral de Coahuila

12 Octubre 2020

Tecnológico de Monterrey

IEC Instituto Electoral de Coahuila

Agenda

Recomendaciones

Pruebas Caja Negra

Pruebas de Análisis de Vulnerabilidades

Pruebas de Ataque DOS

Pruebas para Firma Digital (SHA256) de archivos

Recomendaciones

En el servidor 10.50.1.171 se sugiere cerrar el puerto TCP/4567 el cual se encontró abierto y no se logro identificar una aplicación correspondiente para este puerto.

El servidor 10.50.1.154 se cambio por el 10.50.1.171, por lo que la base de datos no estará ahí. Se sugiere que este sea apagado

Se sugiere abrir un ticket de evento con los proveedores de telecomunicaciones durante el evento para facilitar la comunicación en caso de que se tenga que generar algún reporte

Se sugiere abrir un ticket con el proveedor de CASB para facilitar la pronta respuesta. Los proveedores de estos servicios en la nube tienden a ser estrictos en los tiempos por lo que se recomienda revisar con ellos la forma de establecer un canal directo de comunicación para agilizar los tiempos de respuesta en caso de una eventualidad de ataques de negación de servicio

Pruebas Caja Negra

Prueba	Criterio Aceptación	Resultado	Comentarios
7.1 Condiciones iniciales de pruebas APP Móvil			
7.2 Acceso a la aplicación	Entrar exitosamente a la aplicación con usuario/clave asignado	ACEPTADO	• Se dio acceso a la aplicación de manera correcta. Esta se instalo de un apk que compartieron
7.3 Registro correcto de Actas	Registrar actas proporcionadas exitosamente	ACEPTADO	• Se logro registrar las actas asignadas
7.4 Registro incorrecto de Actas	Tener pantalla para revisar el acta sin permitir el acceso a capturar acta	ACEPTADO	• Las actas que se llenan de forma incorrecta se validan y se evita su captura
7.5 Tomar la Foto desde el Teléfono	Tener la foto escaneada en una resolución “legible”	ACEPTADO	• Se revisaron las actas recibidas por teléfono y llega correctamente, visible y permite su lectura para la catpura de datos.
7.6 Transmisión del App al Sitio central			
7.6.1 Comunicaciones entre el APP y el sitio central	Pruebas de alcance con un 90% de efectividad (ICMP)	ACEPTADO	• Se encontró conectividad por encima del 90%. Queda Pendiente agregar la evidencia para el 4/Octubre en el 2º simulacto.
7.6.2 Corte de Comunicaciones entre el APP y el sitio central	Acta en sección de Seguimiento marcada como pendiente.	ACEPTADO	• El corte se llevo acabo el día 11 de Octubre en el 3er simulacro y se probó la entrad del sitio alterno la cual se hizo en un periódo de 3.40 minutos para los sitios de captura y 5.10 minutos para los de escaneo.
7.7 Seguimiento de actas	Acta en sección seguimiento para re-envio posterior a corte de comunicaciones	ACEPTADO	• En el corte de comunicaciones y servidores, se interumbpió la conexión y fue posible restaurar la captura hasta terminar al 100% de las actas pendientes y detenidas por el corte.
7.8 Validación de conexión segura entre el APP y el sitio central	**<PENDIENTE REVISAR CONEXIONES SSL EN RUTEADOR O FW>**	ACEPTADO	• Los teléfonos que hacen de escanners se conectan vía SSL al sitio de web. Los escaners de plancha, se conectan por IPSEC site-to-site.
7.9 Validación de passwords	Passwords deben ser 8 caracteres, con mezcla de letras (mayusculas, minúsculas, números y caracterés especiales)	ACEPTADO	• Se proporciono un usuario con su clave de 12 caracteres en total mezclando números, mayúsculas y mínusculas. Todos los usuarios son nombrados (no hay genéricos) • Se verifico que no se pueda usar mas de 12 caracteres (se encuentra topado el acceso en el APP)
7.10 Validación en sitio central de recepción del acta (Recepción del acta)	Timestamp de recepción del acta debe ser la misma que se recibió del teléfono.	ACEPTADO	• La BD tiene como parte de los elementos de las imágenes, el timestamp en que se envía.

Pruebas Caja Negra

Prueba	Criterio Aceptación	Resultado	Comentarios
8 Casos de prueba CATD con Multifuncional			
8.1 Condiciones iniciales de pruebas Multifuncional	Conexión hacia CCV en IPSEC	ACEPTADO	• El multifuncional se conecta por medio de una VPN site to site
8.2 Enlace del Multifuncional hacia sitio central	Pruebas de alcance con un 90% de efectividad (ICMP)	ACEPTADO	• El equipo que recibe en el sitio central tiene bloqueado la respuesta al ping por lo que no se pudo medir el tiempo de respuesta, pero se logro la conectividad y escanear los 1000 puertos
8.3 Validación de conexión segura entre el Multifuncional y sitio central	Configuración del Ruteador o FW para el multifuncional	ACEPTADO	• Los teléfonos que hacen de escanners se conectan vía SSL. Los escaners de plancha, se conectan por IPSEC site-to-site.
8.4 Validación de passwords	Passwords deben ser 8 caracteres, con mezcla de letras (mayusculas, minúsculas, números y caracterés especiales)	ACEPTADO	• Se proporciono un usuario con su clave de 12 caracteres en total mezclando números, mayúsculas y mínusculas. Todos los usuarios son nombrados (no hay genéricos) • Se verifico que no se pueda usar mas de 12 caracteres (se encuentra topado el acceso en el APP)
8.5 Escanear el acta	Archivo en formato PDF o gráfico en el multifuncional con nombre único para ser enviado al centro de procesamiento.	ACEPTADO	• El acta es recibida y visible para la captura de datos en el centro de captura
8.6 Comunicación para envío desde el CATD			
8.6.1 Envío del acta desde el APP	Archivo de acta deberá residir, después del envío en la BD del centro de procesamiento	ACEPTADO	• El acta queda resguardada en la BD (de donde es asignada a un operador para la captura de los resultados
8.6.2 Interrupción en el envío del acta desde el APP	Acta no queda en el centro de procesamiento y se conserva en el multifuncional para su envío posterior	ACEPTADO	• Aunque se resguarda e el dispositivo para su envío para su envío posterior, no fue posible probarlo dado que no se hizo el simulacro de interrupción de comunicaciones. Al ser enviada la foto desaparece del dispositivo. • Pendiente EVIDENCIA
8.6.3 Validación en sitio central de recepción del acta (Recepción del acta)	Recepción posterior a caída de enlace del archivo encolado (no enviado) en el multifuncional	ACEPTADO	• El CCV pudo volver a capturar en 3.40 minutos solictiando nuevas actas. Los CATD's vuelven a enviar actas después de 4.10 minutos una vez que se arrancan los sistemas en el sitio alterno

Pruebas Caja Negra

Prueba	Criterio Aceptación	Resultado	Comentarios
8.7 Validación en sitio central de recepción de acta (caso de doble envío del acta)	Timestamp de recepción del acta debe ser la misma que se recibió del teléfono	ACEPTADO	• La BD de captura, tiene configurado el timestamp de recepción y el hash que genera la imagen al ser escaneada
8.8 Obtención del acta por equipo de capturistas del PREP (acta única)		ACEPTADO	• El usuario hace la solicitud de acta par que se le asigne. Al recibir una es capturada con los campos que existen en la plataforma.
8.9 Obtención del acta por equipo de capturistas del PREP (acta repetida)		ACEPTADO	• Ver prueba 9.5 del proceso de resolución actas duplicadsa en mesa de control donde se resolucona este tipo de incidentes,
9 Datos de captura para Calcúlo y Publicación			
9.1 Condiciones Iniciales de Captura	Base de datos en limpio	ACEPTADO	• Se corrió proceso para reiniciar la BD y poder iniciar el proceso de captura con una BD en limpio.
9.2 Captura de valores requeridos del Acta en la Base de datos del SIPRE	Valores mínimos requeridos deben estar para su captura en la interfase del SIPRE	ACEPTADO	• Los campos permitidos son los mínimos requeridos que vienen en el ACTA.
9.3 Datos a Calcular	Los datos mínimos para calcular en la interfase del SIPRE deben reflejarse.	ACEPTADO	• Los datos se iban presentando en el dashboard mientras se iban capturando por la sala de operaciones del centro de captura. Pendiente anexar evidencia
9.4 Datos a Publicar	Deben presentar los datos a publicar ques e mencionan en el documento de plan de pruebas como entregables mínimos.	ACEPTADO	• Los datos se presentaron en el portal de pruebas durante el ejercicio de simulacro.
9.5 Corrección de actas duplicadas	Documentar proceso mediante le cual se validan las actas duplicadas	ACEPTADO	• La mesa de control permite validar actas repetidas, valores inconsistentes en caso de que lleguen al centro de captura y validación. Esta mesa se encuentra en el CCV para esto. Esta mesa no solicita actas para captura, solamente hace las validaciones cuando se requieren.

Análisis de Vulnerabilidades

Prueba	Criterio Aceptación	Resultado	Comentarios
4.1 Diseño y Arquitectura de Red			
4.1.1 Diseño jerarquico de la red	Validar diagrama muestra estructura y modelo de red.	ACEPTADO	• El diagram de red que se entrego se documenta en la sección de anexos
4.1.2 Redundancia en conexión	Verificar que haya conexión alterna de salida del centro captura.	ACEPTADO	• Existe una conexión alterna por un proveedor (ESPECTRO). El primario es ALESTRA. Los enlaces estan en tándem por lo que al caer uno, el otro toma el enlace
4.1.3 Direccionamiento adecuado y eficiente	Confirmar que el direccionamiento este segmentado por funciones, alcances y responsabilidades.	ACEPTADO	• Se confirmó que se cuenta con segmentación de red, permitiendo separación de servicios y usuarios.
4.1.4 Acceso controlado a redes en sitios de captura	Validar que el acceso a los closets de telecom debe estar controlado y asegurado.	ACEPTADO	• Se pudo validar que el acceso al site principal en el sitio del IEC se encuentra bajo llave y con control de acceso Hay que pasar 3 controles par llegar al site del IEC
4.2 Validación de versiones sin vulnerabilidades críticas	Verificar que las versiones de los switches y routers no deben presentar vulnerabilidades críticas ni altas.	ACEPTADO	• Los switches no son administrables • Los Firewalls CISCO ASA (que es en donde está conectado la WAN) tiene la versión 9.12(2)4. Se encontró una vulnerabilidad pero no aplica para el IEC dado que el problema esta sobre el protocolo IKEv1 y se esta usando IKEv2
4.3 Soporte manual a infraestructura	Confirmar que se cuenta con contratos de soporte, así como soporte en sitio y vía telefónica para soporte.	ACEPTADO	• Se confirmó que hay dos firewalls en redundancia a donde llegan los enlaces de los dos proveedores. Se confirma que hay contrato de mantenimiento
4.4 Validación de estaciones de captura			
4.4.1 Acceso con privilegios mínimos	Validar que se cuenta con acceso del usuario solo a lo que requiere.	ACEPTADO	• Los usuarios tienen identificación única en la red para cada estación, no tene salida a Internet, no tienen acceso a disco o USB por lo que no pueden tener interacción externa para la instalación de software y solo tiene instalado el browser que da acceso al sistema de captura
4.4.2 Servicios habilitados en estaciones de captura	Validar la lista de servicios abiertos en estaciones captura.	ACEPTADO	• Se pudo validar que debido a que las máquinas sólo tienen acceso a red local del PREP no es factible usar otros servicios compartidos, sólo locales.

Análisis de Vulnerabilidades

Prueba	Criterio Aceptación	Resultado	Comentarios
4.4.3 Vulnerabilidades en las estaciones de captura	Validar que no haya lista de vulnerabilidades de nivel crítico y alto en las estaciones de captura.	ACEPTADO	• La versión del sistema operativo esta parchada y actualizad al día en que se escaneo por lo que no hay al momento vulnerabilidades o advertencias que haya sobre el sistema.
4.4.4 Acceso de las estaciones de captura	Confirmar que las estaciones de captura solo tienen la aplicación para captura de elecciones.	ACEPTADO	• Se confirmó que las estaciones de captura sólo tienen acceso a red local del PREP y se encuentra asociada al usuario con que se firman a la aplicación de captura
4.4.5 Acceso a la infraestructura de comunicaciones	Confirmar que hay bloqueo de puertos TELNET, WEB, si no es así, debe haber lista de acceso. Acceso solo vía SSH.	ACEPTADO	• Se confirmó que los puertos están cerrados y sólo existe conexión a la red local, no cuentan con salida a internet.
4.4.6 Puertos dedicados	Confirmar que se tiene habilitado Port Blocking.	ACEPTADO	• Los switches no proveen esta función, pero verifico que no hay puertos de red RJ45 disponibles en la sala de captura. A los capturistas se les solicita guardar sus equipos móviles y las redes inalámbricas solo dan acceso a Internet y solo son accesibles bajo solictud al equipo de sistemas.
4.5 Controles de seguridad de Operaciones en la red del PREP			
4.5.1 Seguridad en Operaciones: Administración de la Capacidad	Validar la existencia de control de aplicaciones y/o enlace desborde para consumo ancho banda.	ACEPTADO	• El dimensionamiento se monitoreoa desde estaciones de monitoreo, pero se encuentra dimensionado correctamente. El desborde de tráfico se da en caso de caída del enlace primario (Alestra/Axtel) al enlace secundario.
4.5.2 Seguridad en Operaciones: Protección contra malware	Confirmar la existencia de controles para evitar la introducción de malware en la red.	ACEPTADO	• Las computadoras de captura cuentan con herramientas de Antivirus y firewall del sistema operativo instalado. Adicionalmente los USBs estan deshabilitados así como la salida a Internet
4.5.3 Seguridad en Operaciones: Bitácora de eventos	Validar la existencia de bitácoren de eventos del ambiente de red LAN y WAN.	ACEPTADO	• Existe tanto bitácora de eventos de la BD que se esta monitoreando como monitoreo por estaciones de Graphana para verificar gráficamente el uso de infraestructura.
4.5.4 Seguridad en Operaciones: Restricciones para instalación de SW	Validar la existencia de controles para evitar instalación de SW no permitido en estaciones de trabajo.	ACEPTADO	• Se pudo validar que no hay salida a Internet ni a dispositivos USB o de disco en las estaciones de captura por lo que no se puede tener acceso a SW externo para capturar. Aparte hay supervisores de línea que vigilan que no haya personas con equipos y/o móviles o tratando de instalar aplicaciones en los sistemas de captura.

Análisis de Vulnerabilidades

Prueba	Criterio Aceptación	Resultado	Comentarios
4.6 Controles de comunicaciones seguras			
4.6.1 Comunicaciones Seguras: Controles de la Red	Confirmar que el área de captura y almacenamiento deberá estar segregado de otras áreas de TI.	ACEPTADO	Se confirmo que las áreas de captura se encuentran separadas física (en un centro de datos) y lógicamente (en una subred sin acceso mas' que los puertos permitidos de captura) de la red donde están las aplicaciones de captura.
4.6.2 Comunicaciones Seguras: Seguridad de los servicios de red	Validar la existencia de control de protocolos no permitidos. Tener una lista de servicios/protocolos permitidos.	ACEPTADO	Se tiene acceso solo a protocolos permitidos por las aplicaciones de captura, SSH y bases de datos: TCP22, TCP80, TCP514, TCP3306, TCP53, TCP21
4.6.3 Comunicaciones Seguras: Segregación en redes	Confirmar que se tiene un esquema de direccionamiento con evidencia de la segregación.	ACEPTADO	Se verifico el esquema de direccionamiento donde se muestra clara separación de los servidores y del ambiente de captura del IEC
4.6.4 Comunicaciones Seguras: Transferencia de información	Confirmar que se tienen canales seguros de transmisión de estaciones de captura hasta sistema.	ACEPTADO	Se tiene un servicio con certificado interno, aparte que los servicios no salen hacia Internet son todos servicios internos hacia servidores con SSL (Secure Socket Layer)
4.7 Escaneo a infraestructura de computo	Confirmar que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	ACEPTADO	Se valido en el escaneo al 26/Sept que no hay vulnerabilidades altas ni críticas. Solo se encontraron medias y bajas. Reporte se encuentra en la sección de anexos.
4.8 Escaneo de infraestructura de comunicaciones	Validar que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	ACEPTADO	No se ha presentado ninguna vulnerabilidad de nivel crítico en la infraestructura. Solo se encontró una vulnerabilidad de nivel medio relacionada con el protocolo IKEv1 la cual no aplica para el IEC ya que se esta utilizando el protocolo IKEv2

Análisis de Vulnerabilidades

Prueba	Criterio Aceptación	Resultado	Comentarios
4.9 Revisión de configuración de infraestructura de comunicaciones			
4.9.1 Revisión de configuración Switches LAN	Revisar la configuración de la infraestructura de switches cumpliendo los requerimientos de mejores prácticas y proporcionar recomendaciones sobre este	ACEPTADO	Los switches LAN no son configurables
4.9.2 Revisión de configuración Router	Validar la configuración de la infraestructura de router cumpliendo los requerimientos de mejores prácticas	ACEPTADO	La arquitectura contempla el uso de los FW's como conexión hacia la WAN y así mantenerla aislada de la red del IEC
4.9.3 Revisión de configuración Firewall	Validar la configuración de la infraestructura de Firewall cumpliendo los requerimientos de mejores prácticas	ACEPTADO	Se reviso la configuración del FW. Solo se compartió la parte de túneles y sesiones dado que hay configuraciones mas orientadas a la conectividad del IEC y no fue compartida la totalidad.

Firma Digital de Archivos

Prueba	Criterio Aceptación	Resultado	Comentarios
2 Firma de aplicación en SHA256	realizar la firma del binario y sus componentes para obtener una firma basada en el protocolo SHA256	PENDIENTE	Esta prueba quedo pendiente de ejecutare debido a las observaciones que el INE compartirá con el IEC y que se habrán de acatar. Una vez que se cumplan se ejecutará la firma y cierre de documentos
Coincidencia de la firma digital	Firma digital obtenida deberá coincidir con la generada previamente	PENDIENTE	Esta prueba quedo pendiente de ejecutare debido a las observaciones que el INE compartirá con el IEC y que se habrán de acatar. Una vez que se cumplan se ejecutará la firma y cierre de documentos
3 Inicialización de la base de datos	La base de datos es arrancada e inicializada. Esta debe mostrar las tablas en valores 0 o “null”	ACEPTADO	Se valido el procedimiento con el cual la base de datos esta en ceros. Este proceso se corre desde el administrador para reiniciarla y con esto poder empezar con el proceso de captura de actas

Pruebas para DOS

Prueba	Criterio Aceptación	Resultado	Comentarios
Ataque volumétrico por TCP - SYN FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina sin afectación al uso del ancho de banda..	**SUSTITUIDA**	• La prueba no fue ejecutada por no tener los permisos de ejecución para este tipo de pruebas sobre infraestructura de terceros (el proveedor de CASB es CLOUDFLARE) • Se confirma la existencia de los filtros por parte de CLOUDFLARE para la contención de ataques de SYN-FLOOD. (https://www.cloudflare.com/es-es/learning/ddos/syn-flood-ddos-attack/) • Se establecieron recomendaciones al INE sobre el manejo de comunicación con el proveedor durante el evento
Ataque volumétrico por UDP - DNS AMPLIFICATION	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina sin afectación al uso del ancho de banda..	**SUSTITUIDA**	• La prueba no fue ejecutada por no tener los permisos de ejecución para este tipo de pruebas sobre infraestructura de terceros (el proveedor de CASB es CLOUDFLARE) • Se confirma la existencia de los filtros por parte de CLOUDFLARE para la contención de ataques de DNS AMPLIFICATION (https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/) • Se establecieron recomendaciones al INE sobre el manejo de comunicación con el proveedor durante el evento
Ataque volumétrico por ICMP - ICMP FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina sin afectación al uso del ancho de banda..	**SUSTITUIDA**	• La prueba no fue ejecutada por no tener los permisos de ejecución para este tipo de pruebas sobre infraestructura de terceros (el proveedor de CASB es CLOUDFLARE) • Se confirma la existencia de los filtros por parte de CLOUDFLARE para la contención de ataques de ICMP-FLOOD (https://www.cloudflare.com/es-es/learning/ddos/ping-icmp-flood-ddos-attack/) • Se establecieron recomendaciones al INE sobre el manejo de comunicación con el proveedor durante el evento
Ataque en la capa de aplicación – SLOWRIS ATTACK	Asegurar que las sesiones arrancadas simulando baja velocidad, deberán cerrarse por falta de respuesta en tiempos adecuados para no sobresaturar el servidor de WEB.	**SUSTITUIDA**	• La prueba no fue ejecutada por no tener los permisos de ejecución para este tipo de pruebas sobre infraestructura de terceros (el proveedor de CASB es CLOUDFLARE) • Se confirma la existencia de los filtros por parte de CLOUDFLARE para la contención de ataques de SLOWRIS ATTACK. • La versión de servidor de web en uso es la 2.4.29 e incluye el modulo que permite ocuparse de este tipo de ataques. Este módulo esta presente desde la versión 2.2: – mod_reqtimeout Limita en tiempo la cantidad de requerimientos a recibir • Se establecieron recomendaciones al INE sobre el manejo de comunicación con el proveedor durante el evento